UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/618,861	07/14/2003	Eric Balard	TI-34921	6971

23494 7590 05/27/2010

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
05/27/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ERIC BALARD and ALAIN CHATEAU

Appeal 2009-006613
Application 10/618,861
Technology Center 2400

Decided: May 25, 2010

Before LEE E. BARRETT, STEPHEN C. SIU, and
DEBRA K. STEPHENS, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-46. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

The Invention

The disclosed invention relates generally to a secure computing system (Spec. 1, ¶ [0004]).

Independent claim 1 is illustrative:

> 1. A method of securing access to resources in a computing device, comprising the steps of:
>
> storing an encrypted access code in a memory location within the computing device;
>
> receiving a password to access the resources;
>
> encrypting the password to produce a encrypted password;
>
> comparing the encrypted password to the encrypted access code;
>
> allowing access to the resources if the encrypted access code matches the encrypted password.

The References

The Examiner relies upon the following references as evidence in support of the rejections:

Lohstroh	US 5,768,373	Jun. 16, 1998
Gray	US 6,268,788 B1	Jul. 31, 2001
Debry	US 6,341,521 B1	Nov. 06, 2001
Reddy	US 6,824,051 B2	Nov. 30, 2004 (filed Jun. 07, 2002)

The Rejections

1. The Examiner rejects claims 1, 4-7, 10-13, 15-21, 23, 24, 26-28, 30, 33-38, 40, 41, and 43-45 under 35 U.S.C. § 102(e) as being anticipated by Gray.

2. The Examiner rejects claims 2, 3, 8, 9, 29, and 46 under 35 U.S.C. § 103(a) as being unpatentable over Gray and Lohstroh.
3. The Examiner rejects claims 14, 25, 31, 32, and 42 under 35 U.S.C. § 103(a) as being unpatentable over Gray and Reddy.
4. The Examiner rejects claims 22 and 39 under 35 U.S.C. § 103(a) as being unpatentable over Gray and Debry.

ISSUE 1: claims 1-45

Appellants assert that Gray fails to disclose "'storing an encrypted access code in a memory location within the computing device'" (App. Br. 5-6) or a system "receiving a password to access resources in the computing device" (App. Br. 6).

Did the Examiner err in finding that Gray discloses storing an encrypted access code in memory within a computing device and allowing access to resources if the encrypted access code matches the encrypted password?

ISSUE 2: claims 4, 10, 16, 19, 20, 33, 36, and 37

Appellants assert that Gray fails to disclose "a memory that cannot be externally modified" (App. Br. 7), a "particular memory location [that] is disabled, such that the data cannot be overwritten" (App. Br. 10), and portions of memory that "are not externally accessible and are not modifiable" (App. Br. 11).

Did the Examiner err in finding that Gray discloses memory that cannot be externally modified, a memory location that is disabled such that data cannot be overwritten, and memory that is not externally accessible and is not modifiable?

ISSUE 3: claim 5 and 11

Appellants assert that Gray fails to disclose "allowing access to testing resources if the encrypted access code matches the encrypted password" (App. Br. 8).

Did the Examiner err in finding that Gray discloses allowing access to testing resources if the encrypted access code matches the encrypted password?

ISSUE 4: claims 6 and 12

Appellants assert that Gray fails to disclose "allowing access to change system parameters" (App. Br. 8) or allowing "access to system parameters" (App. Br. 14).

Did the Examiner err in finding that Gray discloses allowing access to system parameters and access to changing system parameters?

ISSUE 5: claims 5, 13, 15, 16, 20, 24, 30, 33, 37, and 41

Appellants assert that Gray fails to disclose a "memory location . . . within a processing system in the computing device" (App. Br. 8), "a memory subsystem within the processing system" (App. Br. 9), "a

memory subsystem within the computing device" (App. Br. 14), and a memory system that "is external to the processing system but internal to the computing device" (App. Br. 12).

Did the Examiner err in finding that Gray discloses a memory location within a processing system of a computing device, within a memory system of a processing system, external to a processing system and internal to a computing system, and a memory subsystem that is within a computing device?

ISSUE 6: claims 17 and 34

Appellants assert that Gray fails to disclose "a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array" (App. Br. 10).

Did the Examiner err in finding that Gray discloses read only memory and random access memory coupled to a memory array?

ISSUE 7: claims 21 and 38

Appellants assert that Gray fails to disclose a key "generated by a random number generator internal to the processing system" (App. Br. 11).

Did the Examiner err in finding that Gray discloses an encryption key generated by a random number generator internal to the processing system?

ISSUE 8: claims 26 and 43

Appellants assert that Gray fails to disclose "one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number" (App. Br. 12).

Did the Examiner err in finding that Gray discloses at least one of a test ID, manufacturer's public key, or die identification number stored in an array?

ISSUE 9: claims 14, 25, 31, 32, and 42

Appellants assert that Gray fails to disclose "a baseband processing system" (App. Br. 22) or a "radio frequency (RF) system" (App. Br. 22).

Did the Examiner err in finding that the combination of Gray and Reddy discloses or suggests a baseband processing system and a radio frequency system?

FINDINGS OF FACT

The following Findings of Facts (FF) are shown by a preponderance of the evidence.

1. Gray discloses an "authenticating system 10 comprises a computer 12" (col. 4, ll. 9-10) that has a "verification unit 20 [that] has a slot 32 which receives a card 34" (col. 4, ll. 21-22).
2. Gray discloses that a "password is entered . . . and provided to the verification unit 20" (col. 6, ll. 52-54), which "encrypts and temporarily stores the password in RAM 66 . . . then proceeds to read

the encrypted password stored in the card 34 . . . and compares the encrypted password received from the card 34 with the encrypted password stored in RAM 66" (col. 6, ll. 56-60).

3. Gray discloses that upon "comparison of the passwords, the verification unit 20 generates a status signal . . . and forwards it to the computer 12" (col. 6, ll. 61-63). "If the status signal indicates that the authentication was successful, i.e., the encrypted password from the keyboard 16 matches the encrypted password from the card 34, the computer 12 grants execution control of the application software to the operator" (col. 6, l. 65 – col. 7, l. 2).
4. Gray discloses that "applications software programs" (executing on the computer system) include "local security programs" (col. 4, ll. 49-53).
5. Gray discloses that an "operator may . . . alter the application program(s) unlocked through the use of the password" (col. 7, ll. 5-7).
6. Gray discloses a computing system (Fig. 2, element 10) and a processor (Fig. 2, element 60).
7. Gray discloses a computing system (Fig. 2, element 10) containing a processor (Fig. 2, element 60).
8. Gray discloses a memory (Fig. 2, element 62) containing ROM (Fig. 2, element 64) and RAM (Fig. 2, element 66) within a computing system or device and an inserted card (Fig. 2, element 34) that contains memory (Fig. 2).

9. Gray discloses that the memory (Fig. 2, element 62) is located within a computer system or device (Fig. 2, element 10) that contains a processor (Fig. 2, element 60).
10. Gray discloses generating "a random number . . . [that] may be used to encrypt messages or other keys" (col. 12, ll. 15-17) and that the "random number thus generated may also be stored in the card 34 and subsequently used to encrypt other keys" (col. 12, ll. 20-22).
11. Reddy discloses computing devices including "a personal computer, hand held computer, PDA, or any other general purpose programmable computer or combination of such devices, such as a network of computers" (col. 6, ll. 31-34).

PRINCIPLES OF LAW

Anticipation

In rejecting claims under 35 U.S.C. § 102, "[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation." *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375 (Fed. Cir. 2005) (citation omitted).

Obviousness

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and

(3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966).

"The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007).

ANALYSIS

Issue 1

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal with respect to Issue 1 on the basis of claim 1 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Claim 1 recites a memory location within a computing device. Claim 7 recites a memory coupled to a processing system. As set forth above, Gray discloses a card that is inserted in a "verification unit" of a computing system (FF 1), the card including a memory. Since the card has memory and the card is inserted into a computer system, we agree with the Examiner that the memory of the card is located "within" the computing device (i.e., "inserted" into the computing device) as recited in claim 1 and that the card is coupled to a processing system of the computing device/system as recited in claim 7 since the card is connected (i.e., "coupled") to the computing system or device.

While Appellants argue that the "card 34 is a peripheral device that is NOT part of verification unit 20" (App. Br. 6), Appellants have not shown

that the card, once inserted into a computing system is somehow not "within" the computing system.

Appellants also argue that Gray fails to disclose a "password to access resources in the computing device" (App. Br. 6). As described above, Gray discloses matching a received encrypted password with a stored encrypted password and allowing access to application software if a match is found (FF 2-3). We construe the term "resources" broadly but reasonably to include an application that executes in a computer system or device. Because Gray discloses providing access to a "resource" (i.e., application) of a computer device or system, we disagree with Appellants' contention that Gray supposedly fails to disclose this feature.

For at least the aforementioned reasons, we find no error in the Examiner's rejection of claims 1 and 7, and claims 2-6 and 8-45, which fall therewith, with respect to Issue 1.

Issue 2

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claims 4, 10, 16, 19, 20, 33, 36, and 37 with respect to Issue 2 on the basis of claim 4 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As described above, Gray discloses authenticating a user based on a comparison between an encrypted password input by the user with an encrypted password stored in memory on a card inserted into the computing system (FF 1-3). Since the password received from the user is compared to the stored password for authentication purposes, it would make no sense and

would defeat the purpose to permit the stored password to be altered by an external party. Since the authentication would be ineffective if external parties were permitted to modify the stored password and since Gray does not otherwise disclose that the stored password is in fact changed by an external party, we agree with the Examiner that Gray discloses that the stored password is stored in memory that cannot be externally modified.

In addition, as the Examiner points out, Gray discloses that in at least one embodiment, the system "[locks] and/or permanently [disables] the card 34" (col. 8, ll. 14-15). A locked or permanently disabled card is neither externally modifiable nor accessible.

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 4, and claims 10, 16, 19, 20, 33, 36, and 37, which fall therewith, with respect to issue 2.

Issue 3

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claim 5 and 11 with respect to Issue 3 on the basis of claim 5 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As described above, Gray discloses permitting user access to application programs (FF 1-3) in which the application programs include local security programs (FF 4). We construe security programs broadly but reasonably to include any program that determines an aspect of security. Determining a level of security includes, for example, testing of various scenarios, authentication levels, or security devices. Such testing, when

interpreted broadly but reasonably, includes testing resources such as security resources or devices. Thus, we agree with the Examiner that Gray discloses allowing user access to testing resources.

While Appellants generally argue that Gray supposedly fails to disclose this feature and that the Examiner's determination is supposedly "not supported by fact" (App. Br. 8), Appellants nevertheless provide no specific support for these contentions or how Gray's security testing differs from the claimed "testing resources."

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 5, or claim 11, which falls therewith, with respect to issue 3.

Issue 4

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claim 6 and 12 with respect to Issue 4 on the basis of claim 6 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As described above, Gray discloses permitting user access to application programs (FF 1-3) and permitting the user or operator to alter the application programs that are unlocked by the password. Since Gray discloses the user altering the application program and altering the program includes altering parameters within the program, we agree with the Examiner that Gray discloses allowing user access to change system parameters.

While Appellants generally argue that Gray supposedly fails to disclose this feature and that the Examiner's determination is supposedly "not supported by fact" (App. Br. 8), Appellants nevertheless provide no specific support for these contentions or how Gray's disclosure of permitting a user access to alter computer programs differs from the claimed feature of allowing access to system parameters or to change system parameters.

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 6, or claim 12, which falls therewith, with respect to issue 4.

Issue 5

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claims 13, 15, 16, 20, 24, 30, 33, 37, and 41 with respect to Issue 5 on the basis of claim 13 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As described above, Gray discloses a computer device or system that contains a processor and memory (FF 6-9). Appellants provide no specific definition for a "processor," a "processing system," a "memory subsystem," or a "computing device." In the absence of such definitions, we construe these terms broadly but reasonably to include any device or group of devices that processes data (a "processor" or a "processing system"), any entity containing memory (a "memory subsystem"), or any device or group of devices that computes or otherwise manipulates data ("computing device").

Gray discloses a processor and memory within a computing system (FF 6-9). Since a processing system, construed broadly but reasonably, may

include a processor, Gray discloses a processing system (i.e., a computing system that contains a processor) with memory that is "within" the "processing system" (Fig. 2). Since a "processor" may also constitute a "processing system," Gray also discloses an embodiment in which the memory is located external to a processor (i.e., memory 62 is located external to processor 60 – Fig. 2) but within a computing device (Fig. 2, element 10).

Also, Gray discloses a "memory subsystem" (e.g., memory 62 – Fig. 2) that is within a system that processes data (i.e., a "processing system" such as the system 10 or verification unit 20 illustrated in Fig. 2) and within a computing device (i.e., any device that computes or otherwise manipulates data such as system or device 10 illustrated in Fig. 2).

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 13, or claims 15, 16, 20, 24, 30, 33, 37, and 41, which fall therewith, with respect to issue 5.

Issue 6

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claims 17 and 34 with respect to Issue 6 on the basis of claim 17 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As described above, Gray discloses ROM and RAM that is in communication with and connected to memory on a card 34 (FF 8-9). In the absence of an explicit definition in the Specification, we construe the terms "connected to" and "coupled to" broadly but reasonably to be equivalent

terms. Therefore, Gray discloses ROM and RAM (memory subsystem) that is "coupled to" a memory array (i.e., memory on card 34).

Appellants argue that ROM and RAM in Gray "are not 'coupled to a memory array'" (App. Br. 10) but fails to provide a reason for this assertion.

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 17, and claim 34, which falls therewith with respect to issue 6.

Issue 7

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claims 21 and 38 with respect to Issue 7 on the basis of claim 21 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As set forth above, Gray discloses utilizing a random number generator to generate an encryption key (FF 10). In view of this explicit disclosure by Gray, we disagree with Appellants' contention that Gray supposedly fails to disclose this feature.

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 21, and claim 38, which falls therewith with respect to issue 7.

Issue 8

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claims 26 and 43 with respect to Issue 8 on the basis of claim 26 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

As set forth above, Gray discloses storing a password in memory (FF 1-4). Since Appellants provide no explicit definition of the term "test ID" and since the term "test ID" construed broadly but reasonably includes any form of identification (i.e., "ID") associated with a test, we agree with the Examiner that the claimed "test ID" includes a password or personal identification number as a password or personal identification number is an identifier that is "tested" for a match.

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 26, and claim 43, which falls therewith with respect to issue 8.

Issue 9

Based on Appellants' arguments in the Appeal Brief, we will decide the appeal of claims 14, 25, 31, 32, and 42 with respect to Issue 9 on the basis of claim 14 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Appellants argue that it would not have been obvious "to incorporate a baseband processing system in to the device of Gray" or "to incorporate a radio frequency system to the processing system in the device of Gray" because "there is no teaching or suggestion in Reddy for computers requiring RF communication" (App. Br. 22).

However, since Gray discloses authenticating users in a computing system or device (FF 1-3), Reddy discloses computing devices including a hand held computer or PDA which the Examiner finds "utilizes baseband/rf technology" (Ans. 10), and combining a computing system that authenticates

a user (Gray) with a computing system including a PDA that utilizes baseband or RF technology would have entailed no more than the mere combination of known elements performing known functions to achieve an expected result such as devising a computing device or system that includes PDA devices (Reddy) that authenticates users (Gray), we agree with the Examiner that it would have been obvious to one of ordinary skill in the art to have combined the Gray and Reddy references. "The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416.

Appellants argue that it would not have been obvious to combine the Gray and Reddy references (App. Br. 22) but fail to provide any specific arguments demonstrating that the combination of Reddy and Gray would have resulted in anything more than predictable results from a combination of known elements.

For at least the aforementioned reasons, we conclude that the Examiner did not err in rejecting claim 14, and claims 25, 31, 32, and 42 with respect to issue 9.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that the Examiner did not err in:

1. finding that Gray discloses storing an encrypted access code in memory within a computing device and allowing access to resources if the encrypted access code matches the encrypted password (Issue 1),

2. finding that Gray discloses memory that cannot be externally modified, a memory location that is disabled such that data cannot be overwritten, and memory that is not externally accessible and is not modifiable (Issue 2),

3. finding that Gray discloses allowing access to testing resources if the encrypted access code matches the encrypted password (Issue 3),

4. finding that Gray discloses allowing access to system parameters and access to changing system parameters (Issue 4),

5. finding that Gray discloses a memory location within a processing system of a computing device, within a memory system of a processing system, external to a processing system and internal to a computing system, and a memory subsystem that is within a computing device (Issue 5),

6. finding that Gray discloses read only memory and random access memory coupled to a memory array (Issue 6),

7. finding that Gray discloses an encryption key generated by a random number generator internal to the processing system (Issue 7),

8. finding that Gray discloses at least one of a test ID, manufacturer's public key, or die identification number stored in an array (Issue 8), and

9. finding that the combination of Gray and Reddy discloses or suggests a baseband processing system and a radio frequency system (Issue 9).

DECISION

We affirm the Examiner's decision rejecting claims 1, 4-7, 10-13, 15-21, 23, 24, 26-28, 30, 33-38, 40, 41, and 43-45 under 35 U.S.C. § 102(e) and claims 2, 3, 8, 9, 14, 22, 25, 29, 31, 32, 39, 42, and 46 under 35 U.S.C. § 103.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

msc

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265